

## MAT0265 - GRUPOS

### LISTA 2 - EXERCÍCIO 32

PEDRO GIGECK FREIRE - 10737136

(32) Seja  $G$  um grupo. Por automorfismo de  $G$  entende-se um isomorfismo de  $G$  em  $G$ . Seja  $\text{Aut}(G)$  o conjunto de todos os automorfismos de  $G$ .

(a) Mostre que  $\text{Aut}(G)$  é um grupo com operação binária dada pela composição de funções.

VAMOS MOSTRAR que  $\text{Aut}(G)$  possui um elemento neutro.

(i)  $\text{Id}$  (função identidade) é o elemento neutro de  $\text{Aut}(G)$ .

Dirretamente da definição de  $\text{Id}$ .

Seja  $\varphi \in \text{Aut}(G)$

$$\varphi \circ \text{Id} = \text{Id} \circ \varphi = \varphi$$

(ii) Todo elemento tem inverso

Seja  $\varphi \in \text{Aut}(G)$ ,

Como  $\varphi$  é bijetora, existe uma função inversa  $\varphi^{-1}: G \rightarrow G$  tal que

$$\varphi \circ \varphi^{-1} = \varphi^{-1} \circ \varphi = \text{Id}.$$

(Note que  $\varphi^{-1}$  também é bijetora, então  $\varphi^{-1} \in \text{Aut}(G)$ )

(iii)  $\text{Aut}(G)$  é fechado com a operação

Seja  $\varphi, \psi \in \text{Aut}(G)$

Temos que

$$\varphi \circ \psi : G \rightarrow G$$

•  $\varphi \circ \psi$  é sobrejetora:

Seja  $f \in \text{Aut}(G)$ , como  $\psi$  é bijetora, existe  $g \in \text{Aut}(G)$  tal que

$$f = \psi(g)$$

Como  $\varphi$  é bijetora, existe  $h \in \text{Aut}(G)$  tal que

$$g = \varphi(h)$$

Logo  $f = \varphi(\psi(h)) = (\varphi \circ \psi)(h) \in \text{Im}(\varphi \circ \psi)$ .

$\psi \circ \Psi$  é injetora

Sejam  $f, g \in \text{Aut}(G)$  tais que

$$(\Psi \circ \Psi)(f) = (\Psi \circ \Psi)(g) \Rightarrow$$

$$\Psi(\Psi(f)) = \Psi(\Psi(g))$$

Como  $\Psi$  é injetora, então

$$\Psi(f) = \Psi(g)$$

Como  $\Psi$  é injetora, então

$$f = g$$

Logo,  $\Psi \circ \Psi$  é injetora.

De fato  $\Psi \circ \Psi$  é bijetora, então  $\Psi \circ \Psi \in \text{Aut}(G)$ .

Sabemos que a composição de funções é associativa.

Portanto, por (i), (ii) e (iii),  $(\text{Aut}(G), \circ)$  é grupo.

b) Seja  $g \in G$  e defina  $\Psi_g: G \rightarrow G$  por  $\Psi_g(a) = gag^{-1}$  para todo  $a \in G$ .

Mostre que  $\Psi_g \in \text{Aut}(G)$ , para todo  $g \in G$ .

O automorfismo  $\Psi_g$  chama-se automorfismo interno definido por  $g$ .

Seja  $g \in G$  qualquer.

Vamos mostrar que  $\Psi_g$  é um homomorfismo:

Sejam  $a, b \in G$ , temos:

$$\Psi_g(ab) = gag^{-1}abg^{-1} = gag(g^{-1}g)b g^{-1} = (gag^{-1})(gbg^{-1}) = \Psi_g(a)\Psi_g(b).$$

Vamos mostrar que  $\Psi_g$  é isomorfismo, isto é, uma bijeção.

(i)  $\Psi_g$  é injetor

Sejam  $a, b \in G$  tais que

$$\Psi_g(a) = \Psi_g(b)$$

Temos

$$\Psi_g(a) = \Psi_g(b) \Rightarrow$$

$$gag^{-1} = gbg^{-1} \Rightarrow$$

$$g'(gag^{-1})g = g'(gbg^{-1})g \Rightarrow$$

$$(g^{-1}g)a(g^{-1}g) = (g^{-1}g)b(g^{-1}g) \Rightarrow$$

$$a = b.$$

Portanto  $\Psi_g$  é injetor.

(ii)  $\Psi_g$  é sobrejetor

Seja  $b \in G$ .

$$b = (gg^{-1})b(gg^{-1}) = g(g^{-1}b g)g^{-1} = \Psi_g(g^{-1}b g) \in \text{Im}(\Psi_g).$$

Portanto  $\Psi_g$  é sobrejetor.

Logo,  $\Psi_g$  é um homomorfismo bijetor, isto é, um isomorfismo.

Então  $\Psi_g \in \text{Aut}(G)$ .

(c) Seja  $\text{Inn}(G)$  o subconjunto de  $\text{Aut}(G)$  formado por todos os automorfismos internos de  $G$ . Mostre que  $\text{Inn}(G)$  é um subgrupo normal de  $\text{Aut}(G)$ .

Vamos mostrar, primeiro, que  $\text{Inn}(G)$  é subgrupo de  $\text{Aut}(G)$ .

Seja  $e$  o elemento neutro de  $G$  e  $\text{Id}$  o elemento neutro de  $\text{Aut}(G)$ .

Temos que, para todo  $a \in G$ ,

$$\Psi_e(a) = eae = a$$

Portanto  $\Psi_e = \text{Id}$ .

Logo:

$$(i) \text{Id} = \Psi_e \in \text{Inn}(G)$$

Vamos mostrar que a composição de funções é fechada em  $\text{Inn}(G)$ .

Sejam  $\Psi_g, \Psi_h \in \text{Inn}(G)$ , para alguns  $g, h \in G$ .

Temos, para todo  $a \in G$

$$(\varphi_g \circ \varphi_h)(a) = \varphi_g(\varphi_h(a)) = \varphi_g(hah^{-1}) = ghah^{-1}g^{-1}$$

Como  $G$  é grupo, temos que

$$gh \in G \quad \text{e}$$

$$(gh)^{-1} = h^{-1}g^{-1}$$

Portanto

$$ghah^{-1}g^{-1} = (gh)a(h^{-1}g^{-1}) = \varphi_{gh}(a)$$

Ou seja

$$(ii) \quad \varphi_g \circ \varphi_h = \varphi_{gh} \in \text{Inn}(G).$$

Agora, vamos mostrar que  $\text{Inn}(G)$  é fechado para o inverso

Seja  $\varphi_g \in \text{Inn}(G)$  para algum  $g \in G$ .

Vamos mostrar que  $\varphi_{g^{-1}}$  é o inverso de  $\varphi_g$ .

Para todo  $a \in G$

$$\begin{aligned} (\varphi_g \circ \varphi_{g^{-1}})(a) &= \varphi_g(\varphi_{g^{-1}}(a)) = \varphi_g(g^{-1}a(g^{-1})^{-1}) = \varphi_g(g^{-1}a(g^{-1})) = \\ &= g(g^{-1}a(g^{-1}))g^{-1} = (gg^{-1})a(gg^{-1}) = ea \cdot e = a. \end{aligned}$$

Ou seja

$$\varphi_g \circ \varphi_{g^{-1}} = \text{Id}$$

Além disso, analogamente

$$(\varphi_{g^{-1}} \circ \varphi_g)(a) = \varphi_{g^{-1}}(g^{-1}a(g^{-1})) = g^{-1}g^{-1}a(g^{-1}g^{-1}) = a.$$

Portanto

$$\varphi_g \circ \varphi_{g^{-1}} = \varphi_{g^{-1}} \circ \varphi_g = \text{Id}$$

Como o elemento inverso é único, então

$$(iii) (\Psi_g)^{-1} = \Psi_{g^{-1}} \in \text{Inn}(G)$$

Por (i), (ii) e (iii),  $\text{Inn}(G)$  é subgrupo de  $\text{Aut}(G)$ .

Agora, vamos mostrar que  $\text{Inn}(G)$  é subgrupo normal de  $\text{Aut}(G)$ .

Sejam  $\Psi \in \text{Aut}(G)$ ,  $\Psi_g \in \text{Inn}(G)$  (para algum  $g \in G$ ) quaisquer.

Temos que, para todo  $a \in G$

$$\begin{aligned} (\Psi \circ \Psi_g \circ \Psi^{-1})(a) &= \Psi(\Psi_g(\Psi^{-1}(a))) = \Psi(g\Psi^{-1}(a)g^{-1}) = \\ &= \Psi(g)\Psi(\Psi^{-1}(a))\Psi(g^{-1}) \quad (\text{pois } \Psi \text{ é homomorfismo}) \\ &= \Psi(g)a\Psi(g^{-1}) \end{aligned}$$

Sabemos que, como  $\Psi$  é homomorfismo

$$\Psi(g)\Psi(g^{-1}) = \Psi(gg^{-1}) = \Psi(e) = e,$$

$$\text{Logo } (\Psi(g))^{-1} = \Psi(g^{-1})$$

Então

$$\begin{aligned} (\Psi \circ \Psi_g \circ \Psi^{-1})(a) &= \Psi(g)a\Psi(g^{-1}) \\ &= \Psi(g)a(\Psi(g))^{-1} \\ &= \Psi_{\Psi(g)}(a) \end{aligned}$$

Portanto

$$\Psi \circ \Psi_g \circ \Psi^{-1} = \Psi_{\Psi(g)} \in \text{Inn}(G), \text{ para quaisquer } \Psi \in \text{Aut}(G), \Psi_g \in \text{Inn}(G)$$

Isso mostra que  $\text{Inn}(G) \triangleleft \text{Aut}(G)$ .

(d) Mostre que  $\text{Inn}(G) \cong G/\text{Z}(G)$ . (sugestão, considere o homomorfismo

$\Phi: G \rightarrow \text{Aut}(G)$  dado por  $\Phi(g) = \Phi_g$ )

Seja  $\Phi: G \rightarrow \text{Aut}(G)$  uma função dada por

$$g \mapsto \Phi(g) = \Phi_g$$

Onde  $\Phi_g(a) = gag^{-1}$  para todo  $a \in G$ .

- Vamos mostrar que  $\Phi$  é um homomorfismo.

Sejam  $g, h \in G$ .

Temos, para todo  $a \in G$

$$\begin{aligned} (\Phi(gh))(a) &= \Phi_{gh}(a) = gh a (gh)^{-1} = gh a h^{-1} g^{-1} = \\ &= g \Phi_h(a) g^{-1} = \Phi_g(\Phi_h(a)) = (\Phi_g \circ \Phi_h)(a). \end{aligned}$$

Ou seja,

$$\Phi(gh) = \Phi(g) \circ \Phi(h)$$

Portanto  $\Phi$  é homomorfismo.

- Vamos mostrar que  $\text{Ker } \Phi = \text{Z}(G)$

( $\subseteq$ ) Seja  $g \in \text{Ker } \Phi$ , isto é,  $\Phi(g) = \text{Id}$ .

Temos que, para todo  $a \in G$

$$\Phi_g(a) = \text{Id}(a) = a \Rightarrow$$

$$gag^{-1} = a \Rightarrow gag^{-1}g = ag \Rightarrow ga = ag$$

Portanto  $g \in \text{Ker } \Phi \Rightarrow ga = ag \quad \forall a \in G \Rightarrow g \in \text{Z}(G)$ .

( $\supseteq$ ) Seja  $g \in \text{Z}(G)$

Então  $ga = ag \quad \forall a \in \text{Z}(G) \Rightarrow$

$$gag^{-1} = agg^{-1} \Rightarrow \Phi_g(a) = a$$

Portanto  $\Phi(g) = \text{Id}$ . Logo  $g \in \text{Ker } \Phi$ .

Por fim, vamos mostrar que  $\text{Im } \varphi = \text{Inn}(G)$  (direto da definição)

( $\subseteq$ ) Seja  $\varphi(g) \in \text{Im } \varphi$ ,

Temos  $\varphi(g) = \varphi_g \in \text{Inn}(G)$

( $\supseteq$ ) Seja  $\varphi_g \in \text{Inn}(G)$

Temos  $\varphi_g = \varphi(g) \in \text{Im } \varphi$

Agora, pelo teorema do homomorfismo, temos

$$G/\ker \varphi \cong \text{Im } \varphi$$

Como  $\ker \varphi = Z(G)$  e  $\text{Im } \varphi = \text{Inn}(G)$ , então

$$G/Z(G) \cong \text{Inn}(G)$$

Como queríamos demonstrar  $\square$

(e) Mostre que o grupo de automorfismos de um grupo cíclico de ordem finita de ordem  $n$  é isomórfico ao grupo dos elementos inversíveis de  $\mathbb{Z}_n$  (com a multiplicação de  $\mathbb{Z}_n$ ).

Seja  $G$  um grupo cíclico de ordem finita, com  $|G| = n$ .

Vamos definir uma família de funções  $\varphi_m$ , com  $m \in \mathbb{Z}$ :

$\varphi_m: G \rightarrow G$  dada por

$$g \mapsto \varphi_m(g) = g^m \quad \text{para todo } g \in G$$

Agora, vamos provar alguns resultados auxiliares

(i)  $\varphi_m$  é homomorfismo de  $G$  em  $G$ .

Sejam  $a \in G$  um gerador de  $G$ .

Todo elemento de  $G$  pode ser escrito como  $a^i$  para algum  $i \in \mathbb{Z}$ .

Sejam  $a^i, a^j \in G$  quaisquer.

Temos

$$\begin{aligned}\varphi_m(a^i a^j) &= \varphi_m(a^{i+j}) = (a^{i+j})^m = a^{m(i+j)} = a^{mi+mj} = \\ &= a^{mi} a^{mj} = (a^i)^m (a^j)^m = \varphi_m(a^i) \varphi_m(a^j)\end{aligned}$$

Portanto  $\varphi_m$  é homomorfismo.  $\square$

(ii) Se  $\text{mdc}(m, n) = 1$  então  $\varphi_m$  é isomorfismo.

Sabemos (provado no exercício 25 da lista 1) que

$a^m$  é gerador de  $G \Leftrightarrow \text{mdc}(m, n) = 1$ .

• Vamos mostrar que  $\varphi_m$  é injetor

Sejam  $a^i, a^j \in G$  tais que

$$\begin{aligned}\varphi_m(a^i) = \varphi_m(a^j) &\Rightarrow (a^i)^m = (a^j)^m \Rightarrow a^{mi} = a^{mj} \Rightarrow a^{-m} a^{mi} = a^{-m} a^{mj} \\ &\Rightarrow a^i = a^j\end{aligned}$$

• Vamos mostrar que  $\varphi_m$  é sobrejetor ( $G \subseteq \text{Im } \varphi_m$ )

Seja  $g \in G$ .

Como  $\text{mdc}(m, n) = 1$ , então  $a^m$  é gerador, portanto

$$G = \langle a^m \rangle,$$

Então existe  $i \in \mathbb{Z}$  tal que  $g = (a^m)^i = (a^i)^m = \varphi_m(a^i) \in \text{Im } \varphi_m$ .

Logo  $\varphi_m$  é sobrejetor.

Então  $\varphi_m$  é bijutor, com isso,  $\varphi_m$  é um isomorfismo.  $\square$

DEF: Seja  $\Phi_G = \{\varphi_m : \text{mdc}(m, n) = 1\}$

$$(iii) \quad \Phi_G = \text{Aut}(G)$$

( $\subseteq$ ) Seja  $\Psi_m \in \Phi_G$ , i.e.  $\text{mdc}(m, n) = 1$ .

Por (ii)  $\Psi_m$  é isomorfismo, logo é automorfismo.  
Então  $\Psi_m \in \text{Aut}(G)$

( $\supseteq$ ) Seja  $\Psi \in \text{Aut}(G)$  um automorfismo de  $G$ .

Seja  $a \in G$  gerador de  $G$

Temos  $\Psi(a) = a^i$  para algum  $i \in G$ .

Seja  $m$  a ordem de  $a^i$

então  $(e = (a^i)^m) = \Psi(a)^m = \Psi(a^m)$  (pois  $\Psi$  é homomorfismo)

Como  $\Psi$  é isomorfismo,  $a^m = e$ . Logo  $m \geq n$ , mas  $G$  não tem elementos de ordem maior que  $n$ . Portanto  $m = n$  e  $\Psi(a) = a^i$  é gerador.

Então  $\text{mdc}(n, i) = 1$ .

Além disso, para qualquer  $a^j \in G$

$$\Psi(a^j) = (\Psi(a))^j = (a^i)^j = (a^j)^i = \Psi_i(a_j).$$

Então  $\Psi = \Psi_i \in \Phi_G$ . □

Seja  $I(\mathbb{Z}_n)$  o conjunto dos inversíveis de  $\mathbb{Z}_n$ .

Definimos

$$\Psi : I(\mathbb{Z}_n) \rightarrow \text{Aut}(G) \text{ dado por}$$

$$\Psi(\bar{m}) \mapsto \Psi_m. \quad (\text{onde } \Psi_m \text{ está definida no início do exercício})$$

Primeiro, devemos mostrar que  $\Psi$  está bem definida:

(inv) Se  $\bar{m}$  é inversível em  $\mathbb{Z}_n$ , então  $\text{mdc}(m, n) = 1$

(Ou seja  $\bar{m} \in I(\mathbb{Z}_n) \Rightarrow \Psi(\bar{m}) \in \text{Aut}(G) = \Phi_G$ )

Seja  $\bar{m}$  inversível em  $\mathbb{Z}_n$ .

Seja  $d = \text{mdc}(m, n)$ , então

$$d|m \text{ e } d|n \Rightarrow m = qd \text{ e } n = q'd \text{ para alguns } q, q' \in \mathbb{Z}$$

Seja  $\bar{i}$  o inverso de  $\bar{m}$  em  $\mathbb{Z}_n$ , ou seja

$$\bar{m}\bar{i} = \bar{1} \Rightarrow mi \equiv 1 \pmod{n} \Rightarrow$$

$$n | mi - 1 \Rightarrow mi - 1 = q''n, \text{ para algum } q'' \in \mathbb{Z}$$

Substituindo  $m, n$  por  $qd, q'd$ ; temos

$$qdi - 1 = q''q'd \Rightarrow$$

$$qdi - q''q'd = 1 \Rightarrow$$

$$d(qi - q''q') = 1 \Rightarrow$$

$$qi - q''q' = \frac{1}{d}$$

Como o lado esquerdo é inteiro, então  $\frac{1}{d}$  é inteiro, portanto  $d = 1$ .

Isto é  $\text{mdc}(m, n) = 1$ .

Portanto  $\psi_m \in \Phi_G = \text{Aut}(G)$

(Imagem está contida no contradomínio).  $\square$

Outro ponto necessário para mostrar que a função está bem definida é mostrar que a função mapeia cada ponto do Domínio a um único ponto do Contradomínio:

(v) Se  $\bar{i} = \bar{j}$  então  $\psi(\bar{i}) = \psi(\bar{j})$ . (com  $\bar{i}, \bar{j} \in I(\mathbb{Z}_n)$ )

Se  $\bar{i} = \bar{j}$  então  $i \equiv j \pmod{n} \Rightarrow n | i - j \Rightarrow$

$$i - j = qn \text{ para algum } q \in \mathbb{Z} \Rightarrow$$

$$i = qn + j$$

Seja  $a \in G$  gerador.

Então, para qualquer  $a^k \in G$ , temos

$$\begin{aligned}\varphi_i(a^k) &= (a^k)^i = (a^k)^{\frac{qn}{q}n+j} = (a^k)^{\frac{qn}{q}n}(a^k)^j = \\ &= a^{qn}(a^k)^j = (a^n)^{\frac{qn}{q}k}(a^k)^j = e^{qk}(a^k)^j = \\ &= e(a^k)^j = (a^k)^j = \varphi_j(a^k)\end{aligned}$$

Logo,  $\varphi_i = \varphi_j$ .

Isto é,  $\varphi(i) = \varphi(j)$ .

Portanto, por (inv) e (N), de fato,  $\varphi$  está bem definida.

Agora, vamos mostrar que  $\varphi$  é homomorfismo de  $I(\mathbb{Z}_n)$  para  $\text{Aut}(G)$ .

Sejam  $i, j \in I(\mathbb{Z}_n)$ .

Então

$$\varphi(ij) = \varphi(ij) = \varphi_{ij}$$

E, sendo  $a \in G$  gerador, para todo  $a^k \in G$ :

$$\varphi_{ij}(a^k) = (a^k)^{ij} = ((a^k)^j)^i = (\varphi_j(a^k))^i = \varphi_i(\varphi_j(a^k)) = (\varphi_i \circ \varphi_j)(a^k).$$

Portanto

$$\varphi_{ij} = \varphi_i \circ \varphi_j = \varphi(i) \circ \varphi(j)$$

Ou seja

$$\varphi(ij) = \varphi(i) \circ \varphi(j)$$

Então  $\varphi$  é homomorfismo.

Resta mostrar que  $\Psi$  é bijutor.

(vii)  $\Psi$  é injetor:

Sejam  $\bar{i}, \bar{j} \in I(\mathbb{Z}_n)$  tais que

$$\Psi(\bar{i}) = \Psi(\bar{j}) \Rightarrow \Psi_i = \Psi_j$$

Então, para qualquer  $a^k \in G$

$$\Psi_i(a^k) = \Psi_j(a^k) \Rightarrow$$

$$(a^k)^i = (a^k)^j \Rightarrow$$

$$a^{ki} = a^{kj} \Rightarrow$$

$$a^{ki} a^{-kj} = e \Rightarrow$$

$$a^{ki-kj} = e$$

Como  $n$  é a ordem de  $a$ , então (pelo ex 21 da lista 1)

$$n | ki - kj \Rightarrow$$

$$ki \equiv kj \pmod{n} \Rightarrow$$

$$i \equiv j \pmod{n} \Rightarrow$$

$$\bar{i} = \bar{j} \text{ em } \mathbb{Z}_n.$$

□

(viii)  $\Psi$  é sobrejetor ( $\text{Aut}(G) \subseteq \text{Im } \Psi$ )

Seja  $\psi \in \text{Aut}(G)$

Por (vii)  $\psi \in \Phi_G$ , ou seja, existe  $m \in \mathbb{Z}$ , com  $\text{mdc}(m, n) = 1$  tal que

$$\psi = \Psi_m = \Psi(\bar{m}) \in \text{Im } \Psi$$

Portanto, finalmente, concluimos que  $\Phi$  é um homomorfismo bijetor de  $I(\mathbb{Z}_n)$  em  $\text{Aut}(G)$ , um isomorfismo.

Logo, o grupo de automorfismos de um grupo cíclico de ordem finita  $n$  é isomórfico ao grupo dos elementos inversíveis de  $\mathbb{Z}_n$ . ■

(f) Quantos elementos tem o grupo de automorfismos do grupo cíclico de ordem infinita? Que grupo é esse?

Primeiro, vamos mostrar que um grupo cíclico de ordem infinita  $G$  tem apenas dois geradores.

Seja  $a \in G$  gerador.

Seja  $b \in G$  gerador, vamos mostrar que  $b = a$  ou  $b = a'$ .

Temos que  $b = a^i$  para algum  $i \in \mathbb{Z}$ , pois  $a$  é gerador.

E temos  $a = b^j$  para algum  $j \in \mathbb{Z}$ , pois  $b$  é gerador.

$$\text{Logo } a = (a^i)^j = a^{ij} \Rightarrow$$

$$a^{ij}a^{-1} = e \Rightarrow a^{ij-1} = e$$

Como  $a$  tem ordem infinita, então

$$ij-1 = 0 \Rightarrow ij = 1$$

Portanto há apenas duas possibilidades

$i=j=1$ , nesse caso  $a=b$  ou

$i=j=-1$ , nesse caso  $a=b^{-1}$ ,  $b=a'$ .

Com isso provamos que  $G$  tem apenas dois geradores,  $a$  e  $a'$ .

Seja  $\Phi \in \text{Aut}(G)$  um automorfismo de  $G$ .

Temos que, para qualquer  $a^i \in G$

$$\Psi(a^i) = \Psi(a)^i$$

Isso implica que dois automorfismos  $\Psi$  e  $\Phi$  são iguais se e somente se  $\Psi(a) = \Phi(a)$ .

Mas sabemos que um automorfismo deve levar geradores em geradores.  
(Provado na parte (2) do tópico (iii) do item e))

Portanto, existem apenas dois automorfismos de  $G$ :

$$\Psi: G \rightarrow G$$

$$\Psi(g) \mapsto g \quad (\text{onde } \Psi(a) = a \text{ gerador})$$

e

$$\Psi': G \rightarrow G$$

$$\Psi'(g) \mapsto g^{-1} \quad (\text{onde } \Psi'(a) = a^{-1} \text{ gerador})$$

Em suma,  $\text{Aut}(G)$  possui apenas 2 elementos: a identidade e o automorfismo que mapeia os elementos nos seus inversos.

(g) Mostre que o grupo de automorfismos de  $S_3$  é isomórfico a  $S_3$ .

Vamos construir um isomorfismo de  $S_3$  em  $\text{Aut}(S_3)$ .

Usando a notação em abusão a  $D_3$ , vamos denotar

$$S_3 = \{\text{Id}, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$$

Onde

$$\text{Id} = (1) \quad \sigma = (1 \ 2 \ 3) \quad \sigma^2 = (1 \ 3 \ 2)$$

$$\tau = (1 \ 3) \quad \sigma\tau = (2 \ 3) \quad \sigma^2\tau = (1 \ 3)$$

Sabemos que  $Z(S_3) = \{\text{Id}\}$

portanto

$$S_3/Z(S_3) = \{\sigma \{\text{Id}\} : \sigma \in S_3\} = \{\{\text{Id}\}, \{\sigma\}, \{\sigma^2\}, \{\tau\}, \{\sigma\tau\}, \{\sigma^2\tau\}\}$$

Podemos perceber que  $S_3/Z(S_3)$  é isomórfico a  $S_3$ .

Conforme provamos no item (d)

$$\text{Inn}(S_3) \cong S_3/Z(S_3)$$

logo

$$\text{Inn}(S_3) \cong S_3, \text{ pois } S_3/Z(S_3) \cong S_3.$$

Basta provar que  $\text{Aut}(S_3) = \text{Inn}(S_3)$ .

( $\supseteq$ ) Provado no item (b).

( $\subseteq$ ) Seja  $\Psi \in \text{Aut}(S_3)$

Sabemos que  $\Psi$  preserva a ordem dos elementos ( $\text{o}(x) = \text{o}(\Psi(x))$ )

Pois  $\Psi$  é homomorfismo.

Então  $\Psi(\sigma)$  tem ordem 3, portanto

$$\Psi(\sigma) = \sigma \text{ ou } \Psi(\sigma) = \sigma^2 \quad (2 \text{ opções})$$

Da mesma forma

$$\Psi(\tau) = \tau \text{ ou } \Psi(\tau) = \sigma\tau \text{ ou } \Psi(\tau) = \sigma^2\tau. \quad (3 \text{ opções})$$

Portanto, permutando todas as possibilidades, obtemos

que  $|\text{Aut}(G)| = 6$ , mas  $|\text{Inn}(G)| = 6$ ,

como  $\text{Inn}(G) \subseteq \text{Aut}(G)$ , então  $\text{Inn}(G) = \text{Aut}(G)$ .

Portanto  $\text{Aut}(S_3) \cong S_3$ .